AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Sean P. Roberts, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am employed as a Special Agent with the United States Department of Labor, Office of Inspector General, Office of Investigations (DOL OIG OI) in Boston, Massachusetts. I have been a Special Agent with DOL OIG OI since September 2017. I am a graduate of the Criminal Investigator Training Program of the Federal Law Enforcement Training Center in Glynco, Georgia, and have received extensive training in criminal investigation procedures and criminal law. Prior to my tenure with DOL OIG OI, I was a police officer in Massachusetts for approximately six years. I am a graduate of the Massachusetts Police Training Commission Recruit Officer Course and I hold a master's degree in criminal justice from the American Military University. My responsibilities as a Special Agent with DOL OIG OI include investigating fraud, waste, and abuse of Department of Labor programs, as well as Labor Racketeering and Labor Trafficking crimes. During my tenure as a DOL OIG OI Special Agent, I have conducted numerous types of investigations including unemployment insurance fraud, false claims fraud, money laundering, work visa fraud, and human trafficking. During the investigation of these cases, I have participated in the execution of search and arrest warrants.

2. Together with other Special Agents and investigators from DOL OIG OI, the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (DHS ICE HSI), and the Internal Revenue Service, Criminal Investigation, I am currently investigating several individuals, including CHELBE WILLAMS MORAES ("**CHELBE**"); CHELBE's brother, JESSE JAMES MORAES ("**JESSE**"); **JESSE**'s son and

CHELBE's nephew, HUGO GIOVANNI MORAES ("**HUGO**"); **CHELBE**'s daughters CAROLINE DE MORAES PARLEE ("**CAROLINE**") and JANAINA DE MORAES GUALBERTO ("**JANAINA**"); **TONY ANGEL CHACON-GIL a/k/a "MARQUITO" a/k/a "MARCOS CHACON" ("CHACON" or "MARQUITO")**, **EBERSON VANZ**, and others (collectively, the "Target Subjects"), for violations of: Title 8, United States Code, Sections 1324(a)(1)(A)(i) and (B)(1) (knowing that a person is an alien, bringing to or attempting to bring to the United States in any manner whatsoever such person at a place other than a designated port of entry or place other than as designated by the Commissioner, regardless of whether such alien has received prior official authorization to come to, enter, or reside in the United States and regardless of any future official action which may be taken with respect to such alien); 1324(a)(1)(A)(iv) and (B)(1) (encouraging and inducing an alien to come to, enter, and reside in the United States for commercial advantage or private gain, knowing and in reckless disregard of the fact that such coming to, entry, and residence is or will be in violation of law); 1324(a)(1)(A)(v)(I) and (B)(i) (conspiracy to commit and aiding and abetting the previous acts); and 1324(a)(3)(A) (during any 12-month period, knowingly hiring for employment at least 10 individuals with actual knowledge that the individuals are aliens who are unauthorized and have been brought to the United States in violation of this subsection); and Title 18, United States Code, Sections 1956(a)(1)(B)(i) (concealment money laundering); 1956(a)(2)(A) (international promotion money laundering); 1956(h) (money laundering conspiracy); and 1028(a)(2) (knowing transfer of a false identification document knowing that such document was produced without lawful authority); among other offenses (the "Target Offenses").

3. I submit this affidavit in support of an application for a search warrant, under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of Criminal Procedure, to search and seize the Apple, Inc. ("Apple") iCloud account associated with Apple ID hugogmbrazil@gmail.com and associated DSID (the "Target Apple Account").[1] A forensic analysis of **HUGO**'s phone, as defined below, conducted pursuant to a search warrant issued by this Court, has shown that the Apple ID underlying the Target Apple Account is associated with **HUGO**'s phone.

4. There is probable cause to believe that the Target Apple Account contains evidence, fruits, and instrumentalities of the Target Offenses as described in Attachment B to the proposed search warrant.

5. The relevant data for the Target Apple Account is maintained by Apple, which accepts service of process at:

lawenforcement@apple.com.

6. I am a Special Agent and have conducted this investigation working closely with other Special Agents and law enforcement personnel. The facts in this affidavit come from my personal observations and review of records, my training and experience as a DOL-OIG OI Special Agent, and information obtained from other law enforcement personnel and witnesses. Since this

---

[1] Every iCloud account is associated with a specific Apple ID. Apple assigns a unique number called a destination signaling identifier, or "DSID" to each Apple ID, thus allowing the company to maintain the continuity of an account, even when key identifiers, such as e-mail address and name, are changed.

affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known concerning this investigation. I have only set forth the facts necessary to establish probable cause that the Target Subjects have committed one or more of the Target Offenses, and that evidence, fruits, and instrumentalities of the Target Offenses are presently located on and within the premises to be searched.

PROBABLE CAUSE

Execution of Search Warrant on HUGO's Phone

7. On October 3, 2022, based on probable cause established by the Master Affidavit in Support of Search Warrant Applications executed by James M. Staton on October 3, 2022, which is attached hereto and incorporated by reference herein, the Honorable David H. Hennessy, United States Magistrate Judge, issued a warrant to search the Apple iPhone 12 Pro with IMEI 356681110291868 and phone number 781-858-4830 ("**HUGO**'s phone"). Case No. 22-mj-4439-DHH. Agents seized **HUGO**'s phone on October 4, 2022.

8. Forensic agents executing the search warrant on **HUGO**'s phone were able to access only a portion of the data on the phone itself. The data they were able to access, however, showed a "Last Backup Date" of October 3, 2022 at 04:10:34 UTC. I have been informed by forensic agents that this means that the contents of **HUGO**'s phone were backed up to an iCloud account on that date and time. The iCloud account to which **HUGO**'s phone was backed up is the one associated with **HUGO**'s Apple ID, which the forensic agents were able to determine from **HUGO**'s phone is hugogmbrazil@gmail.com. A preservation letter was issued to Apple for this account on October 18, 2022.

Background on WhatsApp

9. Based on my training and experience, I understand that in certain instances iCloud accounts will retain text and/or WhatsApp messages, WhatsApp voice messages (audio files), WhatsApp media/videos/documents sent and received by the iCloud account customer/user. WhatsApp users can use WhatsApp's iCloud backup feature to back up and restore their chat history, media, and messages.

10. Based on my training and experience, I also know that iCloud accounts often contain archived or backed-up third-party application data that may include voice/phone recordings as well as photographs saved by the relevant users. Data from voice/phone recording applications and photographs often provide extremely strong evidence of relationships between individuals. For example, photographs may evidence joint vacations and social interactions, potentially providing insight into the frequency of contacts between individuals.

Background On Apple

11. Apple is a United States company that produces the iPhone, iPad, and iPod Touch—all of which use the iOS operating system—and desktop and laptop computers based on the MacOS operating system.

12. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop software applications ("apps"). The services include e-mail.

13. Apple provides e-mail service to its users through e-mail addresses at the domain names mac.com, me.com, and icloud.com.

14. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the Apple App Store (Mac OS), iTunes (Windows), or via a web browser. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

15. An Apple ID takes the form of the full e-mail address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided e-mail address (often ending in @icloud.com, @me.com, or @mac.com) or an e-mail address associated with a third-party e-mail provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification e-mail" sent by Apple to that "primary" e-mail address provided by the user. Additional e-mail addresses ("alternate," "rescue," and "notification" e-mail addresses) can also be associated with an Apple ID by the user.

16. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of

the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the IP address used to register and access the account, and other log files that reflect usage of the account.

17. Based on my training and experience, I know that Apple maintains records that can link different Apple accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show that a single person, or single group of persons, used multiple Apple accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful in identifying the person or persons who have used a particular Apple account.

18. Based on my training and experience, I know that subscribers can communicate directly with Apple about issues relating to the account, such as technical problems, billing inquiries, or complaints from/about other users. Providers such as Apple typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. In summary, based on my training and experience in this context, and based on my review of other Apple Accounts I have reviewed in this investigation, I believe that the computers of Apple are likely to contain user-generated content such as stored electronic

communications (including retrieved and unretrieved e-mail for Apple subscribers), as well as Apple-generated information about its subscribers and their use of Apple services and other online services. In my training and experience, all that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Apple with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

20. As explained above, information stored in connection with an Apple account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with an Apple account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, text, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Apple can show how and when the account was accessed or used. For example, providers such as Apple typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Apple account access and use relating to the criminal activity

under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the Apple account may indicate its user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

LEGAL AUTHORITY

21. The government may obtain both electronic communications and subscriber information from electronic communications services and remote computer services, including Apple, by obtaining a search warrant. 18 U.S.C. §§ 2703(a) & (b), 2703(c)(1)(A).

22. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a) & (b), regardless of the location of the website hosting company or e-mail provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

23. If the government obtains a search warrant, there is no requirement that either the government or Apple give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

24. This application seeks a warrant to search all responsive records and information under the control of Apple, which is subject to the jurisdiction of this court, regardless of where it has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Apple's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. 18 U.S.C. § 2713.

FOURTEEN-DAY RULE FOR EXECUTION OF WARRANTS

25. Federal Rule of Criminal Procedure 41(e)(2)(A), (B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues the requested warrant, the United States will execute it not by entering the premises of Apple, as with a conventional warrant, but rather by serving a copy of the warrant on Apple and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g),[2] and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

---

[2] Section 2703(g) provides that "[n]otwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service."

26. Based on my training and experience and that of other law enforcement officers, I understand that Apple sometimes produces data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that Apple sometimes produces data that was created or received after this 14-day deadline ("late-created data").

27. The United States does not ask for this extra data or participate in its production.

28. Should Apple produce late-created data in response to the warrant, I request permission to view all late-created data that was created by Apple, including subscriber, IP address, logging, and other transactional data, without further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

29. For these reasons, I request that the Court approve the procedures in Attachment B of the proposed warrant, which sets forth these limitations.

CONCLUSION

30. Based on the information described above, I have probable cause to believe that records and data from the Target Apple Account (as described in Attachment A of the proposed search warrant) contains evidence, fruits, and instrumentalities of the above-listed Target Offenses (as described in Attachment B of the proposed search warrant).

31. The procedures for copying and reviewing the relevant records are set out in

32. Attachment B to the proposed search warrant.

Respectfully submitted,

Sean P. Roberts

SEAN P. ROBERTS
Special Agent, Department of Labor, Office of the Inspector General, Office of Investigations

Sworn to me telephonically
on November 30, 2022

HONORABLE JENNIFER C. BOAL
United States Magistrate Judge

ATTACHMENT A – APPLE

The premises to be searched and seized are: (1) the iCloud account identified as: Apple ID hugogmbrazil@gmail.com (the "Target Account"); (2) other user-generated data stored with this account, including the contents of communications; and (3) associated subscriber, transactional, user connection information associated with the account, as described further in Attachment B. This information is maintained by Apple, Inc., ("Apple"), which accepts service of process at:

Apple Litigation Group
Apple, Inc.
1 Infinite Loop M/S 169-NYJ
Cupertino, CA 05014-2084
lawenforcement@apple.com

ATTACHMENT B – APPLE INC.

I. Search Procedure

A. Within fourteen days of the search warrant's issue, the warrant will be served on Apple, which will identify the accounts and files to be searched, as described in Section II below.

B. Apple will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. Apple will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel may review the account duplicate, even if it is produced more than 14 days after the warrant issues, subject to the following limitations. If data was created by Apple after fourteen days from the warrant's issue ("late-created data"), law enforcement personnel may view any late-created data, including subscriber, IP address, logging, and other transactional data that was created by Apple without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), absent a follow-up warrant.

II. Information to Be Disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of APPLE, including any messages, records, files, logs, documents or information that have been deleted but are still available to APPLE, including all iOS backups and all Apple and third-party application data, or have been preserved pursuant to a request made under 18 U.S.C § 2703(f), APPLE is required to disclose the following information to the government, in unencrypted form whenever available, corresponding to the account or identifier ("Account") listed in Attachment A:

a. *Message content*: For the period between July 1, 2016 and October 3, 2022, the contents of all communications and related transactional records for all APPLE services used by the Account subscriber/user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services), including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies). Contents of all other data and related transactional records for all Apple services used by the Account user including all messages sent to or from, stored/backed-up in draft form in, or otherwise associated with the Account, including all message

content (to include e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services, iOS stored/backed-up voice content), attachments, and header information (specifically including the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message);

b. *Instant Messages*: For the period between July 1, 2016 and October 3, 2022, The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

c. *iCloud Data*: For the period between July 1, 2016 and October 3, 2022, The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, and iCloud Drive. The contents of all other data to include audio files and voice data and related transactional records for all APPLE services and third-party applications/services used by the Account user, including any and all information generated, modified, or stored by user(s) or APPLE in connection with the Account (such as contacts, calendar data, images, videos, notes, audio files, voice notes, third-party application/service data,

Apple and third-party telephone call recorder application data, third-party messenger application data, documents, bookmarks, profiles, device backups, and any other saved information);

d. *Images, videos, audio, documents and files:* All pictures, videos, audio, documents, and files posted and/or stored by the Account user, including metadata and geotags;

e. *Address book information*: All address book, contact list, or similar information associated with the Target Account;

f. *Other stored electronic information*: All records/data and other information stored/backed-up to include Apple and third-party messenger application data such as WhatsApp (text) messages, WhatsApp media (video), WhatsApp voice messages (audio files), WhatsApp documents, and WhatsApp contacts;

g. For the period between July 1, 2016 and October 3, 2022: All APPLE records concerning the online search and browsing history associated with the Account or its users (such as information collected through tracking cookies);

h. For the period between July 1, 2016 and October 3, 2022: All records and other information concerning any document, or other computer files created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

i. All records regarding identification of the Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

j. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access APPLE services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

k. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any APPLE account (including both current and historical accounts) ever

linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

l. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

m. For the period between July 1, 2016 and October 3, 2022: All records of communications between APPLE and any person regarding the Account, including contacts with support services and records of actions taken;

n. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to APPLE (including, but not limited to, the keybag.txt and fileinfolist.txt files);

o. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Account or associated user(s) (but not including confidential communications with legal counsel);

p. *Find My iPhone and Remote Deletion Activity*: All find My iPhone connection logs and Find My iPhone transactional activity for requests to remotely lock or erase or wipe a device;

q. *Service information*: The types of services utilized by the user of the Target Account;

r. *Linked Accounts*: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, Apple ID, or otherwise;

s. *Preserved or backup records:* Any and all preserved or backup copies of any of the foregoing categories of records to include voice data (to include Apple and third-party application voice/call recording data), whether created in response to a preservation request issued pursuant to 18 United States Code, Section 2703(f) or otherwise to include any and all messenger application data to include third-party messenger application data such as WhatsApp; and

t. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

u. Within 14 days of the issuance of this warrant, Apple shall deliver the information set forth above via United States mail, courier, or e-mail to the following:

Sean P. Roberts
Special Agent
U.S. Department of Labor-Office of Inspector General, Office of Investigations
675B New Sudbury Street
Boston, MA 02203
roberts.sean@oig.dol.gov

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

A. Evidence, fruits, or instrumentalities of violations of offenses including alien smuggling in violation of 8 U.S.C. §§ 1324(a)(1)(A)(i) and (B)(1); and §§ 1324(a)(1)(A)(iv) and (B)(1); conspiracy and aiding and abetting the same in violation of 8 U.S.C. § 1324(a)(1)(A)(v)(I) and (B)(i); hiring unauthorized aliens in violation of 8 U.S.C. § 1324(a)(3)(A); money laundering in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(a)(2)(A); and money laundering conspiracy in violation of 18 U.S.C. § 1956(h), including:

B. Evidence pertaining to the following people, entities, physical addresses, telephone numbers, e-mail addresses, websites, and social media accounts:

1. **CHELBE** WILLAMS MORAES (DOB 05/16/1961)
2. Phone number +55 31 9727 3586
3. **JESSE** JAMES MORAES (DOB 01/13/1958)
4. Phone number 781-879-0068
5. **HUGO** GIOVANNI MORAES (DOB 10/22/1979)
6. Phone number 781-858-4830

7. **CAROLINE** DE MORAES PARLEE (DOB 10/05/1988)

8. Phone number 781-608-5201

9. **JANAINA** DE MORAES GUALBERTO (DOB 04/09/1994)

10. Phone number 781-640-3632

11. **TASTE OF BRAZIL**—TUDO NA BRASA, LLC, 414 Main Street, Woburn, MA

12. **THE DOG HOUSE** BAR & GRILL, LLC, 434 Main Street, Woburn, MA (together with **TASTE OF BRAZIL, the RESTAURANTS**);

13. 37 Center Street, Woburn, MA

14. hugogmbrazil@gmail.com

15. hugo@thedoghousewoburn.com

16. 434mainstreet@gmail.com

17. loredanna_18@msn.com

18. carolinemoraesbh@hotmail.com

19. Website, Facebook, and Instagram accounts for **THE DOG HOUSE**

20. Website, Facebook, and Instagram accounts for **TASTE OF BRAZIL**

C. Evidence pertaining to the following topics:

1. Identification of employees of the **RESTAURANTS**, such as a list of employees and job duties, employees' names, aliases, addresses, phone numbers, dates of birth, social security numbers and taxpayer identification numbers, identification documents, and applications and employment

contracts.

2. Employees' immigration and work authorization/verification, such as copies of identification documents provided by or on behalf of employees, documents executed by employees and **RESTAURANTS'** supervisors or managers, documents submitted to federal, state and local authorities, and communications.

3. The **RESTAURANTS'** payroll and scheduling records, such as employees' shift schedules, assigned jobs, time cards, records of hours worked, records of payment in any form *(i.e.*, check, cash, debit card, in-kind, satisfaction of debt, etc.), documents submitted to federal, state, and local authorities, and communications.

D. Evidence pertaining to the payment, receipt, transfer, or storage of money or other things of value by or to any one of the names listed above, including, without limitation:

1. Bank, credit union, investment, money transfer, and other financial accounts;

2. Credit and debit card accounts;

3. Tax statements and returns;

4. Business or personal expenses;

5. Income, whether from wages or investments; and

6. Loans.

E. Evidence pertaining to the travel or whereabouts of **CHELBE** WILLAMS MORAES, **JESSE** JAMES MORAES, **HUGO** GIOVANNI MORAES, **CAROLINE** DE MORAES PARLEE, and **JANAINA** DE MORAES GUALBERTO between July 1, 2016 and the present;

F. Evidence pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;

G. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;

H. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);

I. Evidence of the geographic location of user of the Target Account, as well as the computers or devices used to access the Target Account, with respect to information maintained by the Provider relating to GPS, Wi-Fi, cell site location, and mobile networks;

J. Other e mail or Internet accounts providing Internet access or remote data storage;

K. The existence or location of physical media storing electronic data, such as hard drives, CD or DVD ROMs, or thumb drives;

L. The existence or location of paper print outs of any data from any of the above; and

M. Evidence pertaining to any computer hardware, computer software, mobile phones, or storage media related to the Target Account ("the computer equipment"),

including:

1. evidence of who used, owned, or controlled the computer equipment;
2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the attachment of other computer hardware or storage media;
4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
5. evidence of when the computer equipment was used;
6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
7. evidence pertaining to accounts held with companies providing Internet access or remote storage.

DEFINITIONS

For the purpose of this warrant:

N. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.

O. “Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

P. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

Q. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

R. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

S. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.